Irregular Warfare Center
PRISM Insights

Irregular Threats in Africa: Building Resilience in an Evolving Security Landscape

By Dr. Sandor Fabian and Matthew Heidel

21 September 2026

Dr. Sandor Fabian is a contractor currently serving as the Deputy Regional Adviser for U.S. Africa Command in the Irregular Warfare Center and the IWC Functional Area Networks.

Matthew Heidel is a contractor assigned as an analyst for U.S. Africa Command in the Irregular Warfare Center and IWC Functional Area Networks.

The security environment across Africa has undergone profound changes over the past two decades. While conventional interstate warfare remains relatively rare, African countries increasingly face a broad spectrum of irregular threats that challenge state authority, undermine economic development, and threaten regional stability. These threats extend beyond traditional military concerns, encompassing violent extremism, organized crime, cybercrime, piracy, human trafficking, disinformation, climate-related insecurity, and transnational insurgencies. The threats exploit weak governance, porous borders, rapid urbanization, technological advances, and socioeconomic inequalities.

Unlike conventional military threats, irregular threats are often decentralized, adaptive, and difficult to predict. They are frequently carried out by non-state actors who exploit local grievances while leveraging regional and global networks for financing, recruitment, logistics, and propaganda. Modern irregular warfare also blurs the distinction between peace and conflict, combining political influence, criminal enterprise, cyber operations, and information campaigns to weaken state institutions without necessarily engaging in open warfare.

Africa's diversity means that no single security model applies universally. Security challenges in the Sahel differ significantly from those in the Horn of Africa, the Gulf of Guinea, Southern Africa, or the Great Lakes region. Nevertheless, common patterns emerge that require integrated responses combining military capabilities, effective governance, economic development, international cooperation, and community resilience.

Understanding Irregular Threats

Irregular threats encompass activities conducted by state or non-state actors that seek political, ideological, religious, or economic objectives through unconventional means. These threats often avoid direct confrontation with superior military forces, instead exploiting societal vulnerabilities, weak institutions, and governance gaps.

Irregular threat actors use a variety of techniques, including:

- Asymmetric tactics against stronger opponents.
- Flexible organizational structures.
- Cross-border mobility.
- Heavy reliance on local populations.
- Integration of criminal and political objectives.
- Use of modern technology for communication, establishing influence, and recruitment.
- Exploitation of economic and social grievances.

Rather than existing independently, these threats frequently reinforce one another. Terrorist and criminal organizations may finance themselves through direct illicit mining, taxing artisanal mining, demanding protection money, or kidnapping by demanding ransom. Criminal syndicates may cooperate with insurgent groups to secure smuggling routes, routes that in turn enable terrorist groups to launder money across borders outside of the financial system. Cybercriminals may support financial crimes that indirectly finance extremist networks. Such convergence complicates national security planning and demands whole-of-government approaches.

Violent Extremism and Insurgency

Violent extremist organizations remain among the most significant irregular threats affecting several African regions. Groups affiliated with global jihadist movements, as well as locally rooted insurgencies, continue to exploit governance deficits, ethnic tensions, poverty, and political instability.

The Sahel has become one of the world's most complex security environments. Armed groups exploit vast, lightly governed territories, moving across borders while targeting military installations, government officials, humanitarian workers, and civilians. Local conflicts over land, resources, and identity often intersect with ideological violence, creating prolonged instability. Similarly, insurgencies in parts of East Africa and Central Africa demonstrate how extremist organizations adapt to local conditions. Rather than relying solely on military strength, these groups often seek legitimacy by providing limited governance, dispute resolution, or economic opportunities where state institutions are absent.

Military operations remain necessary to protect populations and disrupt armed groups. However, experience demonstrates that military action alone rarely produces lasting stability. Sustainable security depends upon strengthening governance, improving public services, promoting inclusive political participation, and addressing the socioeconomic drivers that facilitate recruitment into armed movements.

Organized Crime as a Strategic Security Challenge

Transnational organized crime has evolved into one of Africa's most sophisticated security challenges. Criminal organizations increasingly operate across multiple countries, exploiting differences in legal systems, border controls, and institutional capacity.

Major criminal activities include:

- Drug trafficking.
- Illegal mining.
- Wildlife and natural resource trafficking.
- Human trafficking.
- Arms smuggling.
- Fuel smuggling.
- Illegal fishing.
- Counterfeit goods.

These criminal economies generate billions of dollars annually while undermining government revenue and public confidence. In several regions, criminal organizations establish mutually beneficial relationships with corrupt officials, insurgent groups, or local militias. Illegal mining illustrates the convergence between economic crime and security threats. Armed groups often control mining areas, taxing production, or directly manage extraction of precious metals including gold, as well as rare earth minerals, oil, and gemstones. Revenue generated through illicit mineral trade finances weapons procurement, recruitment, and operational activities.

Similarly, maritime crime in the Gulf of Guinea and the Red Sea affects international shipping, energy infrastructure, and regional trade. Although a combination of coordinated naval operations, security cooperation, and improved anti-piracy best practices for shippers have reduced certain forms of piracy in recent years, maritime security remains closely linked to broader issues of governance, unemployment, and coastal development.

Cyber Threats and Digital Vulnerabilities

Africa's rapid digital transformation has created significant economic opportunities while simultaneously expanding the cyber threat landscape. Governments, financial institutions, telecommunications companies, healthcare systems, and energy providers increasingly rely on interconnected digital infrastructure.

Cyber threats affecting African countries include:

- Financial fraud.
- Ransomware attacks.
- Identity theft.
- Phishing campaigns.
- Critical infrastructure attacks.
- Data breaches.
- Election interference.
- Online disinformation.

Cybercrime has become particularly attractive because it offers relatively low operational costs with potentially high financial returns. Criminal groups operate across jurisdictions, making investigation and prosecution difficult. Beyond criminal activity, cyber operations increasingly form part of broader hybrid strategies aimed at influencing political processes or disrupting essential services. As governments digitize public administration and expand e-government services, cybersecurity becomes an essential component of national resilience rather than simply an information technology issue.
Investment in cyber workforce development, legal frameworks, regional cooperation, and public-private partnerships will be critical to improving cyber resilience across the continent.

Border Security and Regional Cooperation

Africa's extensive land borders present both opportunities for regional integration and challenges for national security. Many borders traverse remote terrain where government presence remains limited. Communities frequently maintain longstanding social, cultural, and economic ties that cross national boundaries.

Irregular actors exploit these realities by moving personnel, weapons, finances, and illicit goods across borders with relative ease. No single country can effectively address these challenges independently. Regional organizations and multinational security initiatives have increasingly recognized the importance of intelligence sharing, joint patrols, coordinated border management, and harmonized legal frameworks. Improving border security should not impede legitimate trade and movement. Instead, modern border management emphasizes risk-based approaches that facilitate economic integration while strengthening law enforcement capabilities.

Information Operations

The growing influence of social media has transformed the information environment across Africa. While digital platforms enhance communication and civic participation, they also provide opportunities for malicious actors to spread influence, incite violence, manipulate elections, recruit supporters, and undermine trust in public institutions. Information operations may originate from domestic political actors, extremist organizations, criminal groups, or foreign influence operations. These campaigns often exploit existing ethnic, religious, or political divisions, making them particularly difficult to counter.

Building societal resilience requires more than technological solutions. Media literacy, transparent government communication, independent journalism, and trusted public institutions all contribute to reducing the effectiveness of information manipulation.

Urban Insecurity and the Rise of Criminal Networks

Africa is urbanizing at an unprecedented rate. Almost half of Africans live in urban areas, which will likely double their physical footprint over the next quarter century, creating significant opportunities for economic growth but also introducing new security challenges. Rapid urban expansion often outpaces infrastructure development, public services, and law enforcement capacity, resulting in informal settlements where governance may be weak.

Urban criminal networks exploit these conditions through extortion, armed robbery, narcotics distribution, illegal taxation, kidnapping, and cyber-enabled fraud. In some cities, criminal organizations evolve beyond localized criminal groups into sophisticated organizations capable of influencing local politics, intimidating communities, and infiltrating legitimate businesses. Unlike insurgencies operating in rural areas, urban criminal organizations thrive within densely populated environments where anonymity, complex social networks, and digital communication complicate policing efforts. Increasingly, these groups leverage encrypted messaging platforms, cryptocurrencies, and social media to coordinate operations and launder proceeds from criminal activities.

Urban insecurity also affects investor confidence, tourism, and economic productivity. Businesses incur higher operating costs due to private security expenditures, while governments face increasing demands for policing and judicial reforms. Effective responses require integrated urban planning, youth employment initiatives, community policing, judicial efficiency, and intelligence-led law enforcement.

Technology and Critical Infrastructure: Opportunities and Emerging Risks

Critical infrastructure forms the backbone of national security and economic resilience while the growing pace of technological innovation creates both potential solutions and novel threats. Energy generation, water systems, telecommunications, transportation networks, ports, airports, healthcare facilities, banking systems, and digital infrastructure are all essential for maintaining public services and supporting economic development.

Irregular actors increasingly recognize that attacking critical infrastructure can produce significant political and economic effects without engaging conventional military forces. Cyberattacks against electricity networks, sabotage of pipelines, attacks on telecommunications towers, or disruptions to transportation corridors can have cascading consequences across multiple sectors.

For many African countries, infrastructure protection is complicated by geographic scale, limited maintenance resources, and expanding digital connectivity. As governments invest in smart cities, digital identity systems, and interconnected public services, cyber resilience becomes inseparable from physical security, a risk as governments look to modernize.

Technological innovation is transforming both security operations and irregular threats. Artificial intelligence, unmanned aerial systems, satellite imagery, biometric identification, and big data analytics provide governments with new tools to improve situational awareness, border surveillance, disaster response, and law enforcement.

At the same time, these technologies are increasingly accessible to non-state actors. Commercial drones have been adapted for reconnaissance, smuggling, and attacks. Artificial intelligence can generate convincing content for information operations, automate phishing campaigns, or accelerate cyberattacks, potentially effectively lowering the threshold for non-state or small state actors to enter the information operation or cybercrime space. Criminal organizations use encrypted communications and digital payment systems to reduce their exposure to law enforcement.

Technology should therefore be viewed as neither inherently beneficial nor inherently harmful. Its impact depends on governance, regulatory oversight, institutional capacity, and responsible adoption. African countries have an opportunity to integrate emerging technologies into national security strategies while investing in education, digital literacy, and ethical governance frameworks that ensure innovation supports democratic accountability and human rights.

Intelligence and Early Warning

Timely intelligence remains one of the most effective tools for preventing irregular threats from escalating into crises. Modern intelligence extends beyond military information and increasingly incorporates data from law enforcement, customs authorities, financial regulators, environmental monitoring, cyber threat intelligence, and community reporting. Early warning systems can identify patterns of radicalization, criminal activity, population displacement, resource competition, or cyber intrusions before they develop into larger security incidents.

Community engagement is particularly important in many African contexts. Local leaders, civil society organizations, traditional authorities, and community policing initiatives often possess valuable insights into changing security conditions. Building trust between communities and security institutions encourages the reporting of suspicious activities while improving the legitimacy of state responses. Regional intelligence-sharing mechanisms also play a crucial role. Because many irregular threats operate across borders, intelligence cooperation among neighboring countries enhances the ability to detect and disrupt transnational networks.

Civil-Military Cooperation

Irregular threats frequently affect civilian populations more directly than conventional military conflicts. Consequently, effective responses require close cooperation between military forces, police, intelligence agencies, emergency services, humanitarian organizations, local governments, and the private sector. Civil-military cooperation is particularly important during humanitarian crises, natural disasters, pandemics, and large-scale population displacement. Military organizations often possess logistics, engineering, aviation, and communications capabilities that can support civilian authorities during emergencies.

However, such cooperation should be guided by clear legal frameworks that define roles, responsibilities, and accountability. Civilian leadership and respect for constitutional governance remain fundamental principles in democratic societies. Military support should complement, rather than replace, civilian institutions. Joint planning, interoperable communication systems, and regular multi-agency exercises strengthen preparedness while reducing duplication of effort during crises.

Regional and International Partnerships

Given the transnational nature of irregular threats, no African country can address them in isolation. Regional cooperation has become increasingly important in areas such as intelligence sharing, border security, maritime surveillance, counterterrorism, cybersecurity, and judicial cooperation.

Continental and regional organizations provide platforms for policy coordination, conflict prevention, peace support operations, and capacity building. International partnerships also contribute technical expertise, training, financial assistance, and technological support. These partnerships are most effective when they prioritize African ownership of security strategies. External assistance should strengthen national institutions rather than create long-term dependency. Sustainable security solutions emerge when local knowledge, political leadership, and community engagement guide policy implementation.

Beyond intelligence and security agencies, effective long-term collaboration also requires a degree of intellectual interoperability built around a common understanding of the security environment. Fortunately, there are promising regional efforts to develop the nuanced, common understanding of irregular threats necessary to cooperate on solutions. Private-sector actors also represent essential partners. Telecommunications providers, financial institutions, energy companies, logistics operators, and technology firms own or manage much of the infrastructure upon which national resilience depends. Effective public-private partnerships facilitate information sharing, incident response, and coordinated investment in resilience.

Building National Resilience

Resilience has emerged as a central concept in modern security policy. Rather than focusing solely on preventing every threat, resilience emphasizes the ability of societies to anticipate, withstand, adapt to, and recover from disruptions.

Building resilience requires coordinated investment across multiple sectors:

- **Strengthening governance:** Transparent institutions, accountable public administration, and effective service delivery reduce opportunities for extremist recruitment and criminal exploitation.
- **Economic inclusion:** Expanding employment opportunities, particularly for young people, helps address socioeconomic conditions that irregular actors often exploit.
- **Education and digital literacy:** Improving educational outcomes strengthens critical thinking and reduces vulnerability to disinformation and online radicalization.
- **Professional security institutions:** Well-trained, accountable military, police, and intelligence services improve operational effectiveness while maintaining public trust.
- **Cyber resilience:** Developing national cybersecurity strategies, incident response capabilities, and skilled cyber professionals protects those that increasingly rely on digital economies.
- **Community engagement:** Inclusive governance and meaningful dialogue with local communities improves early warning and strengthen social cohesion.
- **Infrastructure investment:** Resilient transportation, energy, communications, and healthcare systems enhance both economic development and national security.

Strategic Recommendations for African Governments

To address the evolving irregular threat environment, policymakers should consider several strategic priorities.

First, adopt integrated national security strategies that recognize the interdependence of defense, economic development, cybersecurity, climate adaptation, and governance. Second, strengthen regional cooperation through intelligence sharing, joint operations, harmonized legislation, and coordinated border management. Third, expand investment in technology while simultaneously developing regulatory frameworks that address cybersecurity, privacy, and ethical concerns. Fourth, enhance public-private partnerships for the protection of critical infrastructure, recognizing that much of Africa's essential infrastructure is owned or

operated by private entities. Fifth, prioritize prevention alongside response by investing in education, employment, social inclusion, and community resilience. Finally, ensure that security operations remain consistent with constitutional principles, human rights obligations, and the rule of law. Public trust is a strategic asset that strengthens intelligence gathering, community cooperation, and long-term stability.

Conclusion

Irregular threats represent one of the defining security challenges facing African countries in the 21st century. Their complexity lies not only in the diversity of actors involved but also in the interconnected nature of political instability, organized crime, technological change, climate pressures, and socioeconomic inequality.

Conventional military capabilities remain important, but they are insufficient on their own. Effective responses require comprehensive strategies that integrate defense, diplomacy, development, governance, law enforcement, cybersecurity, environmental management, and community engagement. National resilience depends upon institutions that are capable, accountable, and trusted by the populations they serve.

Africa's future security will be shaped by its ability to adapt to an increasingly interconnected threat landscape while harnessing the continent's considerable strengths: a young population, expanding digital innovation, growing regional cooperation, and increasing investment in institutional capacity. By strengthening resilience, fostering collaboration across sectors, and addressing the root causes of insecurity, African countries can reduce the impact of irregular threats while creating the conditions for sustainable peace, prosperity, and inclusive development.

Ultimately, success will not be measured solely by the defeat of individual armed groups or the disruption of criminal networks. It will be measured by the ability of African societies to maintain stability, protect democratic institutions, secure critical infrastructure, and provide citizens with opportunities that reduce the appeal of violence and illegality. In this broader sense, resilience is not simply a security objective; it is a foundation for national development and long-term human security.

The views expressed in this article are those solely of the author and do not reflect the policy or views of the Irregular Warfare Center, the Department of War, or the U.S. Government.